How to Tunnel VNC through SSH on a Windows Computer

SSH tunneling is a flexible and secure mechanism for accessing network services behind a firewall. It can be used for accessing VNC servers in our Faculty from your <u>office PC</u>.

How secure is VNC:

Although VNC encrypts VNC passwords sent over the net, the rest of the traffic is sent as is, unencrypted (for password encryption, VNC uses a DES-encrypted challenge-response scheme, where the password is limited by 8 characters, and the effective DES key length is 56 bits). So using VNC over the Internet can be a security risk.

What you need:

- Have PuTTY program ready. It is a free implementation of SSH for Win32 and UNIX platforms. You can download it from <u>http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html</u> and save it to your local Windows (e.g. C:\Program Files\).
- 2. Create a shortcut to your Desktop.
- Have VNC Viewer program ready. You can download it from <u>http://www.tightvnc.com/download.html</u> and install it to your office PC.
- 4. An account to login to any Linux workstation/PC cluster (Research machine).

To start a VNC server

 Using PuTTY to login to one of the research machines, e.g. "tdgrocks.sci.hkbu.edu.hk" as the host to connect to. First, make a simple SSH connection and start the vncserver on the remote machine: [username@tdgrocks] \$ vncserver

Note: If this is the first time you run vncserver, the software will ask you to select a password for subsequent VNC sessions. Remember to select a password which is difficult to guess.

2. The program will then show the display number on which your desktop is run. For example,

```
New 'tdgrocks.sci.hkbu.edu.hk:3 (username)' desktop is tdgrocks.sci.hkbu.edu.hk:3
```

It means that your session will run on display 3 of server tdgrocks.

Using PuTTY to Build SSH Tunnel on Command line (at your office PC)

- 1. To open an Command Window, click Start -> Run, and then input "cmd"
- 2. At the command prompt (where the PuTTY program is located), e.g.

C:\Program Files\Putty> putty -L 5903:tdgrocks.sci.hkbu.edu.hk:5903

Where putty –L [Source port + displace #]:[destination server]:[destination post + displace #]

- 3. Login to the gateway server (any server running with sshd; in this case, 'tdgrocks.sci.hkbu.edu.hk') when prompted. You can minimize the active PuTTY session and keep the program running.
- 4. Run VNC Viewer on your PC, and enter "localhost:3" as the Computer to connect to. VNC maps display 3 to port 5903, which SSH is tunneling through its own port (port 22).
- 5. You should terminate your VNC session after you have finished your work. To terminate your VNC session running on the UNIX server, run the command

[username@tdgrocks] \$ vncserver -kill :<display #>

(in this case, it is 3. You should see this output: "Killing Xvnc process ID 15783")

<u>Or</u>

Setting up PuTTY and Build SSH Tunnel (at your office PC)

1. Next start to make a second connection, double click the **PuTTY** icon (shortcut) on your desktop to start the program as shown in the following picture:

Lategory:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial 	Basic options for your PuTTY Specify the destination you want to com Host Name (or IP address) tdgrocks.sci.hkbu.edu.hk Connection type: Paw Ielnet Rlogin SS Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: Always Never Only on	session Port 22 SH Serial Load Save Delete clean exit

2. Click on **SSH** subcategory, enable compression and select protocol level 2 as the default for better security:

Category:				
 Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours 	~	Options controlling SSH connections Data to send to the server Remote command: Protocol options Dog't start a shell or command at all Enable compression		
Connection Data Proxy Telnet Rlogin SSH Kex Auth TTY X11		Preferred SSH protocol version: 1 only 1 2 2 2 only Encryption options Encryption cipher selection policy: AES (SSH-2 only) Blowfish 3DES warn below here Arcfour (SSH-2 only) DES		
Tunnels Bugs Serial	~	Enable legacy use of single-DES in SSH-2		

3. Next, click **Tunnels** and input the **Source port** and **Destination** as shown below:

(In general, a VNC client communicates with a VNC server by connecting to TCP port <5900 + display no> on the UNIX server. In this case, your VNC server is running on tdgrocks.sci.hkbu.edu.hk:3, your VNC client communicates with the VNC server by connecting to TCP port (5900 + 3 =) 5903 on server tdgrocks.)

😵 PuTTY Configuration 🛛 🔀					
Category:					
Category. Keyboard Bell Features Window Appearance Behaviour Translation Colours Connection		Options controlling SSH port forwarding Port forwarding Local ports accept connections from other hosts Remote ports do the same (SSH-2 only) Forwarded ports: Remove			
Data Proxy Telnet Rlogin SSH Kex Auth TTY X11 X11 Bugs		Add new forwarded port. Source port 5903 Add Destination localhost:5903 Image: Destination Destination Image: Destination localhost:5903 Image: Destination Image: Destination Image: Destination <thimage:< td=""></thimage:<>			
	×				
About		<u>Upen</u> <u>C</u> ancel			

4. Click **Add**, the results are displayed like this:

Pully Configura	tion	
Category:		
Category: Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours	^	Options controlling SSH port forwarding Port forwarding Local ports accept connections from other hosts Remote ports do the same (SSH-2 only) Forwarded ports: Remove L5903 localhost:5903
 Connection Data Proxy Telnet Rlogin SSH Kex 		Add new forwarded port: Source port Destination Image: Destinating Image: Des
Auth TTY X11 Bugs Serial	~	

- 5. Next, click **Open**, and login to tdgrocks. Your tunnel is now active.
- 6. Finally, run VNC Viewer on your PC, and enter "localhost:3" as the Computer to connect to. VNC maps display 3 to port 5903, which SSH is tunneling through its own port (port 22).

VNC Viewer : Connection Details					
$\overline{\mathbf{v}}$	Server:	localhos	t:3	~	
	Encryption:	Let Serv	er Choose (Def	ault) 🔽	
<u>A</u> bout.	Optic	ns	ОК	Cancel	

7. You should terminate your VNC session after you have finished your work. To terminate your VNC session running on a UNIX server, run the command

```
[username@tdgrocks] $ vncserver -kill :<display #>
```

(In this case, it is 3. You should see an output similar to this one: "Killing Xvnc process ID 15783")

How to change your VNC password?

To change the VNC password, run

```
[username@tdgrocks]$ vncpasswd
```

on the server.

How to start Gnome Session instead of X over VNC?

Edit the file ~/.vnc/xstartup

At the top you may find the following:

- # Uncomment the following two lines for normal desktop:
- # unset SESSION_MANAGER

```
# exec /etc/X11/xinit/xinitrc
```

Uncomment those two lines as indicated. You can get a Gnome session in your next vnc connection.